數學傳播 50卷1期, pp. 3-5

淺談後量子密碼學近期發展

周 彤

本文於 2025 年 10 月 28 日刊載於中研院訊漫步科研專欄, 作者及中研院訊同意本刊轉載。

量子電腦是基於量子位元 (qubits) 和量子邏輯閘 (quantum gates) 所建構的計算裝置。傳統的位元數量若有 n 個, 有 2^n 種可能的狀態, 但同時只能處在其中一種狀態, 每個邏輯閘也只能對一種狀態做計算。但 n 個量子位元可同時處在這 2^n 個狀態的疊加態, 而量子邏輯閘可同時對這 2^n 個狀態運作。這樣特殊的性質使得量子電腦在解一些特定的問題時能達到傳統電腦無法企及的效率, 也因此近年來量子電腦的發展備受矚目與期待。

密碼學 (cryptography) 是受到量子電腦衝擊的其中一個重要領域。密碼學相較於一些近期熱門的領域如人工智慧, 可能較不爲人所知, 但其實密碼學的發展已有相當長的歷史, 而且現今的網路通訊處處都仰賴密碼系統的保護。知名的傳輸層安全性協定 (Transport Layer Security) 之中就使用了數位簽章和金鑰交換等密碼系統。這些密碼系統讓客戶端可驗證伺服器的身份, 並確保雙方之間傳輸的資料經過加密而無法被第三方竊聽。近年來備受討論的加密貨幣也仰賴數位簽章系統以達到「不可否認性」(non-repudiation) 等安全性質。

有趣的是, 和其他領域不同, 量子電腦對於密碼學的影響是負面的。許多傳統的公開金鑰密碼系統已經被證明可被秀爾演算法 (Shor's algorithm) 快速破解: 在傳統電腦上破解這些公開金鑰密碼系統往往需要指數時間 (exponential time) 的計算量, 然而在量子電腦上使用秀爾演算法的話只要多項式時間 (polynomial time) 的計算量。幸運的是, 目前量子電腦的建構技術尚未成熟, 現有量子電腦的量子位元數量還未達到可實際破解密碼系統的程度。也因此, 密碼學家冀望在大型量子電腦出現之前, 將這些傳統的公鑰密碼系統逐步替換成可抵抗量子電腦攻擊的公鑰密碼系統。而這種類型的密碼系統與相關的研究, 被統稱爲後量子密碼學 (post-quantum cryptography)。值得一提的是, 雖然大衆普遍認爲大型量子電腦的出現仍需一段時間, 但現在在網路傳輸的資料已經受到威脅。這是因爲攻擊者現在就可大量收集以傳統密碼系統加密的資料, 並在未來大型量子電腦出現時, 使用秀爾演算法還原這些資料。換句話說, 後量子密碼系統的需求十分迫切, 不應等到大型量子電腦出現才進行汰換。

美國國家標準技術研究所 (National Institute of Standards and Technology, NIST)

也注意到量子電腦對於密碼系統的威脅, 也因此 NIST 在數年前開始了所謂的後量子密碼標準化過程 (post-quantum cryptography standardization process)。此計畫從 2017 年開始向全世界募集各種後量子密碼系統的提案, 密碼系統的類型包含兩大類, 一類是加密系統 (encryption system) 或密鑰封裝系統 (key encapsulation mechanism), 一類是數位簽章系統 (digital signature)。之後 NIST 開始評估其安全性及效率, 並在每一輪 (一輪約一兩年) 結束時淘汰一些密碼系統。經過數輪的篩選, NIST 最終於 2022 年選出三個簽章系統 DILITHIUM, FALCON, SPHINCS+ 以及一個密鑰封裝系統 KYBER 標準化, 並於 2025 年選擇另一個密鑰封裝系統 HQC 標準化。NIST 也在 2023 年開啟了另一項針對簽章系統的子計畫, 因此未來預計將有更多簽章系統被選擇標準化。

後量子密碼學也是筆者的主要研究領域。筆者的研究內容基本上可分爲密碼系統設計、攻擊、與實作。在密碼系統設計方面, 筆者參與了 Classic McEliece 密鑰封裝系統和 LESS 數位簽章系統等後量子密碼系統的設計, 大幅改進了其公鑰生成的效率以及簽章大小。在密碼系統攻擊方面, 筆者主要針對後量子密碼學中重要的數學難題, 例如二次多變量系統問題 (multivariate quadratic), 改進相關演算法的效率。這種類型的研究可幫助密碼學家量化密碼系統的安全性, 並作爲設計參數的依據。在密碼系統實作方面, 筆者曾建構 CSIDH 等許多密碼系統的快速 constant-time 實作。constant-time 實作的目標是確保密碼系統的計算時間不受機密資料 (如密鑰) 不同影響, 使得攻擊者無法藉由測量計算時間獲得機密資訊, 所以這種類型的實作比一般的實作有更多限制。

雖然美國國家標準技術研究所已選擇了一些後量子密碼系統標準化, 但後量子密碼學仍有許多研究方向值得探索。以下列出一些筆者認爲值得研究的方向。

- 橢圓曲線同源密碼學 (isogeny-based cryptography) 是從 2000 年開始出現的一種後量子密碼學的分支。和傳統的橢圓曲線密碼學不同, 橢圓曲線同源密碼系統使用的是橢圓曲線同源 (isogeny) 相關的數學難題, 也因此無法被秀爾演算法攻擊。橢圓曲線同源密碼學可用來建構加密、簽章和金鑰交換系統, 且這些密碼系統往往擁有非常小的公鑰、簽章大小以及密文, 只是計算上效率較差。若能改進其效率, 橢圓曲線同源密碼系統可能會取代其他類別成爲最熱門的後量子密碼系統類別。
- 「腦內多方計算」(multi-party computation in the head) 是一種可用來建構數位簽章系統的技術。在 NIST 針對簽章系統的子計畫中, 有許多這種類型的簽章系統提案。與一些傳統的簽章系統不同, 此類型的簽章系統不需要仰賴陷門函數 (trapdoor function) 的存在, 也因此攻擊者無法利用陷門函數造成的結構進行攻擊。此外, 這種類型的密碼系統也具備非常小的公鑰。如何進一步改善其簽章大小及計算上的效率, 是一個非常值得深入研究的問題。
- 代數攻擊 (algebraic attacks) 在密碼學中是一種廣泛被使用的攻擊手段。其概念是將密碼

系統轉換爲多變量多項式系統, 並藉由求多變量多項式系統的解, 達到還原私鑰或明文等攻擊目的。代數攻擊的分析經常使用沒有特別結構的多變量多項式系統當作目標, 因爲在這種狀況下的分析通常比較簡單。但即使是在這種狀況下, 仍有一些看似簡單但還未被完全了解的問題。舉例來說, Joux-Vitse 演算法是一個在 2017 年被提出的代數攻擊演算法, 其運作原理並不複雜, 但要如何決定演算法所用的參數目前還沒有定論。此外, 實際的密碼系統常常會被轉換爲有特殊結構的系統, 如何能在存在這些特殊結構的狀況下預測代數攻擊帶來的效果, 似乎也是一個尚未被深入研究的領域。

不可否認, NIST 的後量子密碼標準化過程大幅促進了後量子密碼學的發展, 但筆者認爲這不應該被視爲是終點。密碼學家仍應持續評估現有後量子系統的安全性, 致力於改進其效率, 並持續開發基於各種不同數學難題假設的後量子密碼系統。

—本文作者任職中央研究院資訊科技創新研究中心—